

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-305876

(43)Date of publication of application : 02.11.2000

(51)Int.Cl.

G06F 13/00
G06F 15/177

(21)Application number : 11-117662

(71)Applicant : HITACHI LTD

(22)Date of filing : 26.04.1999

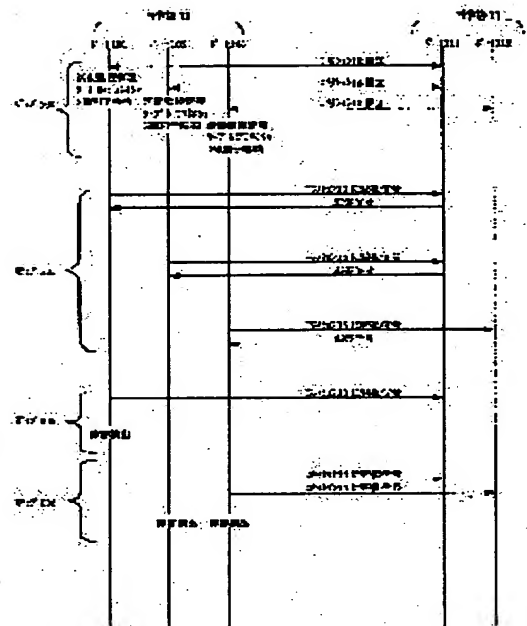
(72)Inventor : MURAI KAZUO
SHIMIZU HIDENORI

(54) METHOD FOR MONITORING CONNECTION ACTIVITY

(57)Abstract:

PROBLEM TO BE SOLVED: To decrease frequency in the transmission of monitor signals by sending the monitor signals normally only to some of a plurality of connections with one computer in such a case.

SOLUTION: Connections 13, 14, and 15 are established between computers 10 and 11 and the computer 10 stores connection identifiers in the activity monitor management table corresponding to the IP address of the computer 11 (500). Then the monitor signal is sent normally to one connection selected out of the three connections which are already made with the computer 11 (501). If a fault is detected at the connection 13 (501), the monitor signal is sent even to the connections 14 and 15 which are established with the computer 11 (503). Consequently, the frequency of monitor signal transmission is reduced to 1/n.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

JPO and NCIP I are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] It is the connection activity monitor approach usually characterized by detecting a failure by transmitting a supervisory signal only about some of the connections at the time when two or more connections exist between computers in the connection activity monitor approach of communication system.

[Claim 2] It is the connection activity monitor approach characterized by transmitting a supervisory signal about all the connections established between the computers acting as a failure, and detecting a connection's failure in the connection activity monitor approach according to claim 1 when a failure is detected in one of connections.

[Translation done.]

SP,2000-303870,A [DETAILED DESCRIPTION] 173-8-2

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the connection activity monitor approach of communication system.

[0002]

[Description of the Prior Art] The keep alive of TCP/IP (TransmissionControl Protocol/Internet Protocol) is in one of the connection activity monitor approaches. Keep alive will transmit a supervisory signal, if the data transmitted to a fixed time amount communication link place calculating machine are lost, and it is judged that the connection failure generated the calculating machine which received the supervisory signal when a letter was answered in a reply signal when a connection's condition is normal, and a reply signal was not answered.

[0003] Use of keep alive raises communication link cost in the network charged to a rise of a network load and a packet by transmission and reception of a supervisory signal or a reply signal. Therefore, when it mounts keep alive by RFC1122, the application program is set to be able to choose whether keep alive is performed for every connection.

[0004]

[Problem(s) to be Solved by the Invention] In the communication system used on basic business etc., the activity monitor of a viewpoint to the connection who detects a failure certainly is required, by the conventional approach, will transmit a supervisory signal through all connections, and has the problem that a network load and communication link cost go up.

[0005]

[Means for Solving the Problem] Since a connection failure is mainly generated with a network out of order or a computer failure, when two or more connections are established among one computer, the need of performing an activity monitor through all connections is low. Therefore, when a connection [finishing / establishment] is managed and two or more connections exist among one computer, a supervisory signal is transmitted only about some of the connections at the time, and it usually reduces the count of transmission of a supervisory signal. When a failure is detected through one of connections, a supervisory signal is transmitted about all the connections established between the computers acting as a failure, and failure detection in all connections is realized.

[0006]

[Embodiment of the Invention] Hereafter, the example of this invention is explained.

[0007] Drawing 1 is drawing showing the example of a configuration of the network in the example of this invention. The computer 10 is connected with the computer 11 through the network 12. A connection 13, a connection 14, and a connection 15 are connections all established from the computer 10, TCP port 101 of a computer 10 and TCP port 102 are connected with TCP port 111 of a computer 11, and TCP port 103 of a computer 10 is connected with TCP port 112 of a computer 11.

[0008] Drawing 2 is the block diagram of a computer. In drawing 2, a computer consists of the supervisory-control section 21 and the protocol processing section 23. The protocol processing section 23 performs communications processing, such as release of establishment of a

connection, data transfer, and a connection. The signal-processing section 24 in the protocol processing section 23 performs transmission and reception of a supervisory signal and a reply signal. The supervisory-control section 21 controls transmission of a supervisory signal using the signal-processing section 24. The activity monitor managed table 22 is a table which manages a connection [finishing / establishment], and exists per IP address of a communication link place computer.

[0009] As shown in drawing 2 , the activity monitor managed table 22 consists of a computer stored in the IP address storing field 221 which stores the IP address of a communication link place computer, and the IP address storing field 221, and a monitor candidate list 222 which stores a connection's [finishing / establishment] connection identifier.

[0010] Drawing 3 and drawing 4 are the flow charts showing processing of the supervisory-control section 21 and the signal-processing section 24, respectively.

[0011] Next, actuation of each part of drawing 2 is explained using the flow chart of drawing 3 and drawing 4 .

[0012] In drawing 3 , if the protocol processing section 23 establishes a connection, connection establishment will be notified to the supervisory-control section 21 (step 300), and the supervisory-control section 21 will search the activity monitor managed table 22 corresponding to the IP address of a communication link place calculating machine with reference to the IP address storing field 221 (step 301). A connection identifier is registered into the tail of the monitor candidate list 222 when retrieval is successful (step 302) (step 304). When a corresponding activity monitor managed table does not exist but retrieval goes wrong, an activity monitor managed table is newly generated, the IP address concerned is set as the IP address storing field 221 (step 303), and a connection identifier is registered into the monitor candidate list 222.

[0013] A time-out is notified to the supervisory-control section 21 at fixed spacing (for example, 60 seconds). If a time-out is notified, from the monitor candidate list 222 of each activity monitor managed tables 22, every one connection who is a no-transmission state will be chosen, and the supervisory-signal transmitting directions to the selected connection will be performed in the signal-processing section 24 (step 305, step 306, step 307). How to choose from the monitor candidate list 222 the connection who performs supervisory-signal transmitting directions is shown in the flow chart of drawing 6 .

[0014] Drawing 6 is shown about how to choose equally the connection who performs supervisory-signal transmitting directions. First, the connection identifier of the head of the monitor candidate list 222 is moved to the tail of a list (step 600). Next, it judges whether the connection of the head of the monitor candidate list 222 is a no-transmission state (step 601), and if it is a no-transmission state, supervisory-signal transmitting directions will be given to the connection (step 602). If it is not a no-transmission state, the connection identifier of the head of the monitor candidate list 222 will be moved to the tail of a list (step 600).

[0015] It repeats until the connection of a no-transmission state finds the above processing. However, when the connection who is a no-transmission state does not exist on the monitor candidate list 222, supervisory-signal transmitting directions are not performed. A connection's connection identifier chosen as the head of the monitor candidate list 222 by the above processing is registered, and the connection who is a no-transmission state can be chosen equally. How to choose the connection to whom the condition of all the connections on a monitor candidate list is judged, and the communication link is not most given for a long time besides the above-mentioned selection approach etc. can be considered.

[0016] In drawing 4 , if the signal-processing section 24 receives the above-mentioned supervisory-signal transmitting directions, a supervisory signal is transmitted to the directed connection, and in order to supervise a reply signal, a watchdog timer will be started (step 400, step 401, step 402).

[0017] If a reply signal is received, the signal-processing section 24 will stop a watchdog timer, and will perform a normal completion report in the supervisory-control section 21 (step 403, step 404, step 405). The supervisory-control section 21 does not transmit a supervisory signal about others and a connection, when a normal completion report is received (step 308).

[0018] When the time-out of a watchdog timer is notified to the signal-processing section 24, connection release processing according to (step 406) and a TCP protocol is performed (step 407), and the notice of a failure of the connection concerned is performed in the supervisory-control section 21 (step 408). The supervisory-control section 21 deletes the connection identifier of the connection acting as [list / 222 / of activity monitor managed tables 22 which correspond when the notice of a failure is received (step 309) / monitor candidate] a failure (step 310), and performs the supervisory-signal transmitting directions to all the connections stored in the monitor candidate list 222 in the signal-processing section 24 (step 311).

[0019] The protocol processing section 23 will notify a connection release to the supervisory-control section 21 and the signal-processing section 24, if a connection is released. If a connection release is notified to the supervisory-control section 21, a connection identifier will be deleted from the monitor candidate list 222 of corresponding activity monitor managed tables 22 (step 312). If a connection release is notified to the signal-processing section 24, a watchdog timer will be stopped when the connection concerned is supervising (step 409, step 410).

[0020] Next, the sequence in the configuration of drawing 1 is explained using drawing 5. In addition, the case where drawing 5 detects a failure by the computer 10 is shown. If a connection 13, a connection 14, and a connection 15 are established between a computer 10 and a computer 11, a computer 10 stores a connection identifier in the activity monitor managed table corresponding to the IP address of a computer 11 (step 500).

[0021] Usually, a supervisory signal is transmitted to one connection who chose by the approach shown in the flow chart of drawing 6 among three connections [finishing / a calculating machine 11 and establishment] at the time (step 501). If a failure is detected through a connection 13 (step 502), a supervisory signal will be transmitted also about the connection 14 and connection 15 who have been established between computers 11 (step 503). The failure detection in all connections becomes possible by the above processing.

[0022] In this example, when two or more connections are established between the same computers and n connections are established between the same computers in order to transmit a supervisory signal to coincidence only through one connection, compared with the time of transmitting a supervisory signal, the count of supervisory-signal transmission can be reduced to $1/n$ through all connections as usual. Moreover, since it is possible to shorten transmitting spacing of a supervisory signal to 1 conventional/ n , without making the count of transmission of a supervisory signal increase, it is also possible to detect a failure at an early stage conventionally by shortening transmitting spacing of a supervisory signal.

[0023]

[Effect of the Invention] Since according to this invention the count of transmission of a supervisory signal was reduced when two or more connections were established between the same computers, a network load required for failure detection and communication link cost are mitigable.

[Translation done.]

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the example of a configuration of the network of this invention.

[Drawing 2] It is drawing showing the example of a configuration of the computer of this invention.

[Drawing 3] It is the flow chart of the supervisory-control section in an example.

[Drawing 4] It is the flow chart of the signal-processing section in an example.

[Drawing 5] It is drawing showing an example of the sequence diagram of the activity monitor in an example.

[Drawing 6] It is a flow chart showing the selection approach of the connection who performs the monitor in an example.

[Description of Notations]

10 — A computer, 11 — 101 A computer, 102,103,111,112 — TCP port, 12 — A network, 13, 14, 15 — A connection, 21 — Supervisory-control section, 22 — An activity monitor managed table, 221 — An IP address storing field, 222 — During a monitor, connection identifier storing field, 223 — An established connection identifier storing field, 23 — Protocol processing section, 24 — The signal-processing section, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309,310,311,312 — Each processing step of a flow chart, 400, 401, 402, 403, 404, 405, 406, 407,408,409,410 — Each processing step of a flow chart, 500,501,502,503 — Each processing step of a sequence diagram, 600,601,602 — Each processing step of a flow chart.

[Translation done.]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-305876

(P2000-305876A)

(43) 公開日 平成12年11月2日 (2000.11.2)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 13/00	3 5 1	C 0 6 F 13/00	3 5 1 N 5 B 0 4 5
15/177	6 7 6	15/177	6 7 6 F 5 B 0 8 9

審査請求 未請求 請求項の数 2 O L (全 9 頁)

(21) 出願番号 特願平11-117662

(22) 出願日 平成11年4月26日 (1999.4.26)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 村井 和男

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア事業部内

(72) 発明者 清水 英則

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア事業部内

(74) 代理人 100075096

弁理士 作田 康夫

Fターム(参考) 5B045 JJ02 JJ12 JJ14

5B089 GA01 GB02 HA01 JB17 KA07

KC28 KC41 MC02

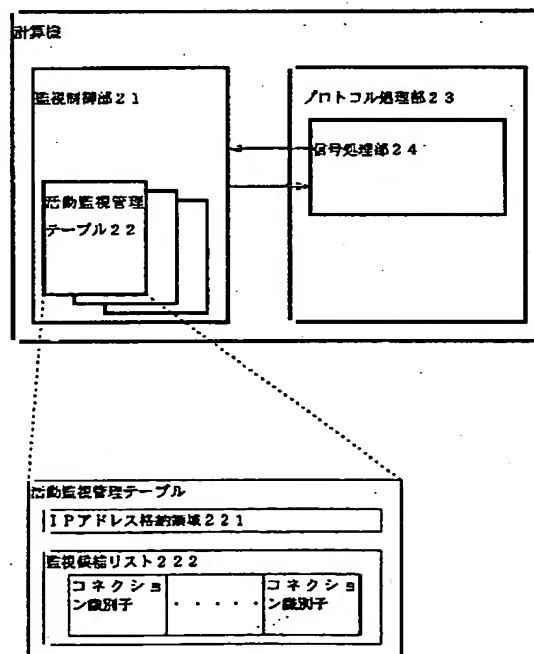
(54) 【発明の名称】 コネクション活動監視方法

(57) 【要約】

【課題】 確立済みの全コネクションで障害を検出する場合には、全コネクションで監視信号を送信する必要があり、障害検出によるネットワーク負荷及び通信コストが上昇する。

【解決手段】 一つの計算機との間に複数のコネクションが確立された場合、一部のコネクションについてののみ監視信号を送信する。

図2



【特許請求の範囲】

【請求項1】通信システムのコネクション活動監視方法において、計算機間に複数のコネクションが存在する場合、通常時はその一部のコネクションについてのみ監視信号を送信することで障害を検出することを特徴とするコネクション活動監視方法。

【請求項2】請求項1記載のコネクション活動監視方法において、いずれかのコネクションにおいて障害を検出したときは、障害となった計算機との間に確立している全コネクションについて監視信号を送信し、コネクションの障害を検出することを特徴とするコネクション活動監視方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は通信システムのコネクション活動監視方法に関する。

【0002】

【従来の技術】コネクション活動監視方法の一つにTCP/IP (Transmission Control Protocol/Internet Protocol) のキープアライブがある。キープアライブは、一定時間通信先計算機に対し送信するデータがなくなると監視信号を送信し、監視信号を受信した計算機はコネクションの状態が正常である場合応答信号を返信し、応答信号が返信されない場合はコネクション障害が発生したと判断する。

【0003】キープアライブを使用すると、監視信号や応答信号の送受信によりネットワーク負荷の上昇、及びパケットに対して課金するネットワークにおいて通信コストが上昇する。よって、RFC1122によりキープアライブを実装する場合は、アプリケーションプログラムが各コネクション毎にキープアライブを行うか否かを選択できるように定められている。

【0004】

【発明が解決しようとする課題】基幹業務等で使用する通信システムにおいては、障害を確実に検出する観点からコネクションの活動監視は必要であり、従来の方法では全コネクションで監視信号を送信することになり、ネットワーク負荷及び通信コストが上昇するという問題がある。

【0005】

【課題を解決するための手段】コネクション障害は、主にネットワーク障害か計算機障害で発生するため、一つの計算機との間に複数のコネクションが確立している場合、全コネクションで活動監視を行う必要性は低い。よって、確立済みのコネクションを管理し、一つの計算機との間に複数のコネクションが存在する場合、通常時はその一部のコネクションについてのみ監視信号を送信し、監視信号の送信回数を削減する。いずれかのコネクションで障害を検出した場合は、障害となった計算機と

の間に確立している全コネクションについて監視信号を送信し、全コネクションでの障害検出を実現する。

【0006】

【発明の実施の形態】以下、本発明の実施例を説明する。

【0007】図1は本発明の実施例におけるネットワークの構成例を表す図である。計算機10は計算機11とネットワーク12を介して接続されている。コネクション13、コネクション14、コネクション15はいずれも計算機10から確立したコネクションであり、計算機10のTCPポート101、TCPポート102は、計算機11のTCPポート111と接続され、計算機10のTCPポート103は計算機11のTCPポート112と接続されている。

【0008】図2は計算機の構成図である。図2において、計算機は監視制御部21とプロトコル処理部23から構成される。プロトコル処理部23は、コネクションの確立、データ転送、コネクションの解放等の通信処理を行う。プロトコル処理部23内の信号処理部24は、監視信号、応答信号の送受信を行う。監視制御部21は、信号処理部24を使用して監視信号の送信を制御する。活動監視管理テーブル22は、確立済みのコネクションを管理するテーブルであり、通信先計算機のIPアドレス単位に存在する。

【0009】図2に示すように活動監視管理テーブル22は通信先計算機のIPアドレスを格納するIPアドレス格納領域221、IPアドレス格納領域221に格納されている計算機と確立済みのコネクションのコネクション識別子を格納する監視候補リスト222から構成される。

【0010】図3、図4はそれぞれ監視制御部21、信号処理部24の処理を表すフローチャートである。

【0011】次に図3、図4のフローチャートを用いて図2の各部の動作を説明する。

【0012】図3において、プロトコル処理部23はコネクションを確立すると、監視制御部21にコネクション確立を通知し(ステップ300)、監視制御部21は、IPアドレス格納領域221を参照し、通信先計算機のIPアドレスに対応する活動監視管理テーブル22を検索する(ステップ301)。検索が成功した場合(ステップ302)は監視候補リスト222の末尾にコネクション識別子を登録する(ステップ304)。対応する活動監視管理テーブルが存在せず検索に失敗した場合は、新たに活動監視管理テーブルを生成し当該IPアドレスをIPアドレス格納領域221に設定し(ステップ303)、監視候補リスト222にコネクション識別子を登録する。

【0013】監視制御部21には一定間隔(例えば60秒)でタイムアウトが通知される。タイムアウトが通知されると、各活動監視管理テーブル22の監視候補リス

ト222から無通信状態であるコネクションを1つずつ選択し、選択したコネクションに対する監視信号送信指示を信号処理部24に行う(ステップ305、ステップ306、ステップ307)。監視候補リスト222から監視信号送信指示を行うコネクションを選択する方法を図6のフローチャートに示す。

【0014】図6は監視信号送信指示を行うコネクションを均等に選択する方法について示してある。まず、監視候補リスト222の先頭のコネクション識別子をリストの末尾に移動する(ステップ600)。次に監視候補リスト222の先頭のコネクションが無通信状態であるか判定し(ステップ601)、無通信状態であればそのコネクションに監視信号送信指示を行う(ステップ602)。無通信状態でなければ監視候補リスト222の先頭のコネクション識別子をリストの末尾に移動する(ステップ600)。

【0015】以上の処理を無通信状態のコネクションが見つかるまで繰返す。ただし、監視候補リスト222上に無通信状態であるコネクションが存在しない場合には、監視信号送信指示は行わない。以上の処理により監視候補リスト222の先頭に選択したコネクションのコネクション識別子が登録され、無通信状態であるコネクションを均等に選択することができる。上記選択方法以外にも監視候補リスト上の全コネクションの状態を判定し最も長い間通信が行われていないコネクションを選択する方法などが考えられる。

【0016】図4において、信号処理部24が上記監視信号送信指示を受けると、指示されたコネクションに監視信号を送信し、応答信号を監視するため監視タイマを起動する(ステップ400、ステップ401、ステップ402)。

【0017】信号処理部24は応答信号を受信すると、監視タイマを停止し、監視制御部21に正常完了報告を行う(ステップ403、ステップ404、ステップ405)。監視制御部21は、正常完了報告を受けた場合他のコネクションについては監視信号は送信しない(ステップ308)。

【0018】信号処理部24に監視タイマのタイムアウトが通知された場合は(ステップ406)、TCPプロトコルに従ったコネクション解放処理を行い(ステップ407)、監視制御部21に当該コネクションの障害通知を行う(ステップ408)。監視制御部21は、障害通知を受けると(ステップ309)対応する活動監視管理テーブル22の監視候補リスト222から障害となったコネクションのコネクション識別子を削除し(ステップ310)、監視候補リスト222に格納されている全てのコネクションに対する監視信号送信指示を信号処理部24に行う(ステップ311)。

【0019】プロトコル処理部23はコネクションを解放すると、監視制御部21と信号処理部24にコネクシ

ョン解放を通知する。監視制御部21にコネクション解放が通知されると、対応する活動監視管理テーブル22の監視候補リスト222からコネクション識別子を削除する(ステップ312)。信号処理部24にコネクション解放が通知されると、当該コネクションが監視中の場合は監視タイマを停止する(ステップ409、ステップ410)。

【0020】次に図5を用いて、図1の構成でのシーケンスを説明する。尚、図5は計算機10で障害を検出する場合について示してある。計算機10と計算機11との間にコネクション13、コネクション14、コネクション15が確立されると、計算機10は計算機11のIPアドレスに対応する活動監視管理テーブルにコネクション識別子を格納する(ステップ500)。

【0021】通常時は計算機11と確立済みの3つのコネクションのうち図6のフローチャートに示した方法で選択した1つのコネクションに対して、監視信号を送信する(ステップ501)。コネクション13で障害を検出すると(ステップ502)、計算機11との間に確立しているコネクション14、コネクション15についても監視信号を送信する(ステップ503)。以上の処理によって全コネクションでの障害検出が可能となる。

【0022】本実施例では、同一計算機間に複数のコネクションが確立されている場合、同時には一つのコネクションだけで監視信号を送信するため、同一計算機間にn本のコネクションが確立しているときは、従来通り全てのコネクションで監視信号を送信したときと比べ、監視信号送信回数を $1/n$ に削減することができる。また、監視信号の送信回数を増加させずに、監視信号の送信間隔を従来の $1/n$ まで短縮することが可能であるため、監視信号の送信間隔を短縮することで、従来より早期に障害を検出することも可能である。

【0023】

【発明の効果】本発明によれば、同一計算機間に複数のコネクションが確立している場合に、監視信号の送信回数を削減したので、障害検出に必要なネットワーク負荷及び通信コストが軽減できる。

【図面の簡単な説明】

【図1】本発明のネットワークの構成例を表す図である。

【図2】本発明の計算機の構成例を表す図である。

【図3】実施例における監視制御部のフローチャートである。

【図4】実施例における信号処理部のフローチャートである。

【図5】実施例における活動監視のシーケンス図の一例を表す図である。

【図6】実施例における監視を行うコネクションの選択方法を表すフローチャートである。

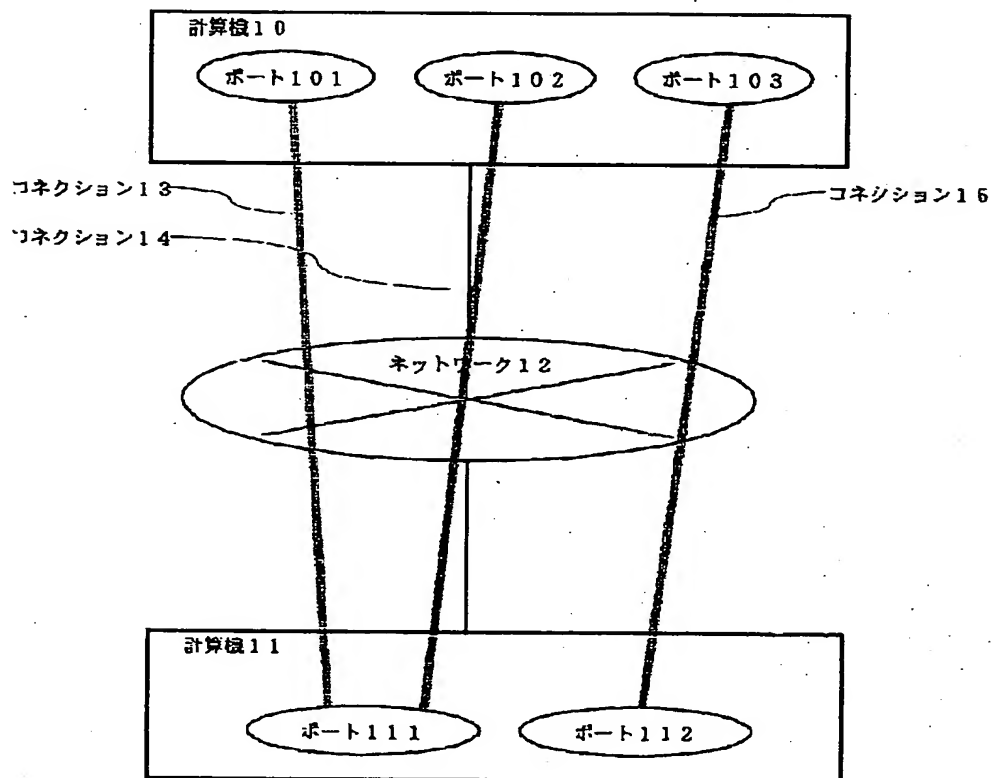
【符号の説明】

10…計算機、11…計算機、101, 102, 103, 111, 112…TCPポート、12…ネットワーク、13, 14, 15…コネクション、21…監視制御部、22…活動監視管理テーブル、221…IPアドレス格納領域、222…監視中コネクション識別子格納領域、223…確立済コネクション識別子格納領域、23…プロトコル処理部、24…信号処理部、300, 301, 302, 303, 304, 305, 306, 30

7, 308, 309, 310, 311, 312…フローチャートの各処理ステップ、400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410…フローチャートの各処理ステップ、500, 501, 502, 503…シーケンス図の各処理ステップ、600, 601, 602…フローチャートの各処理ステップ。

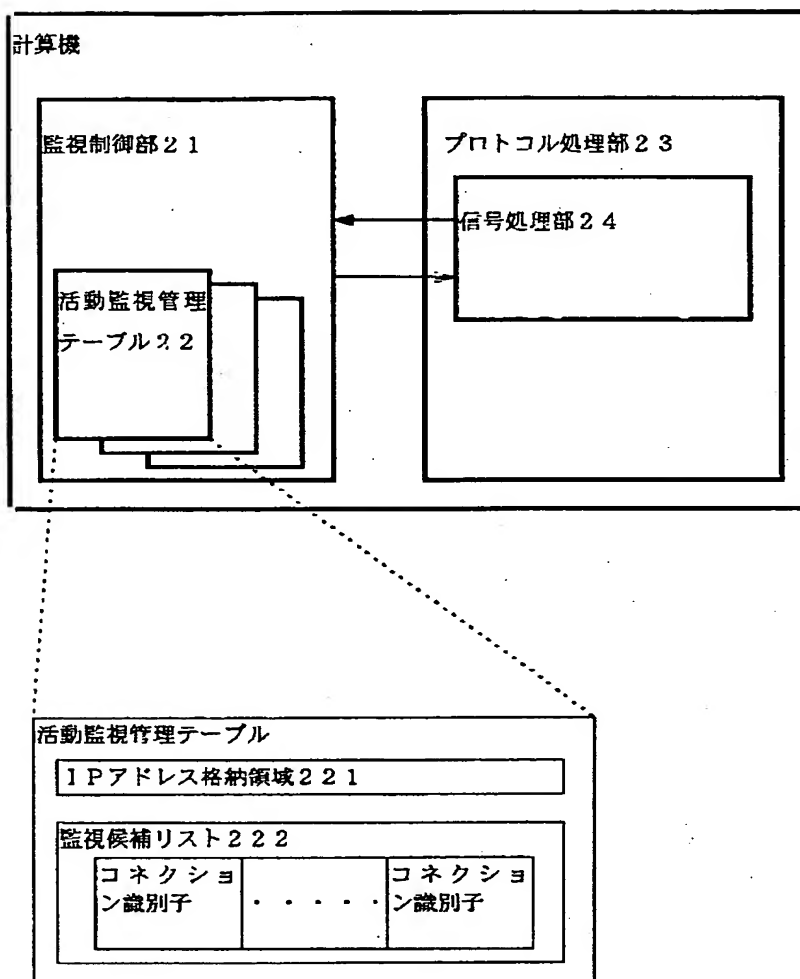
【図1】

図1



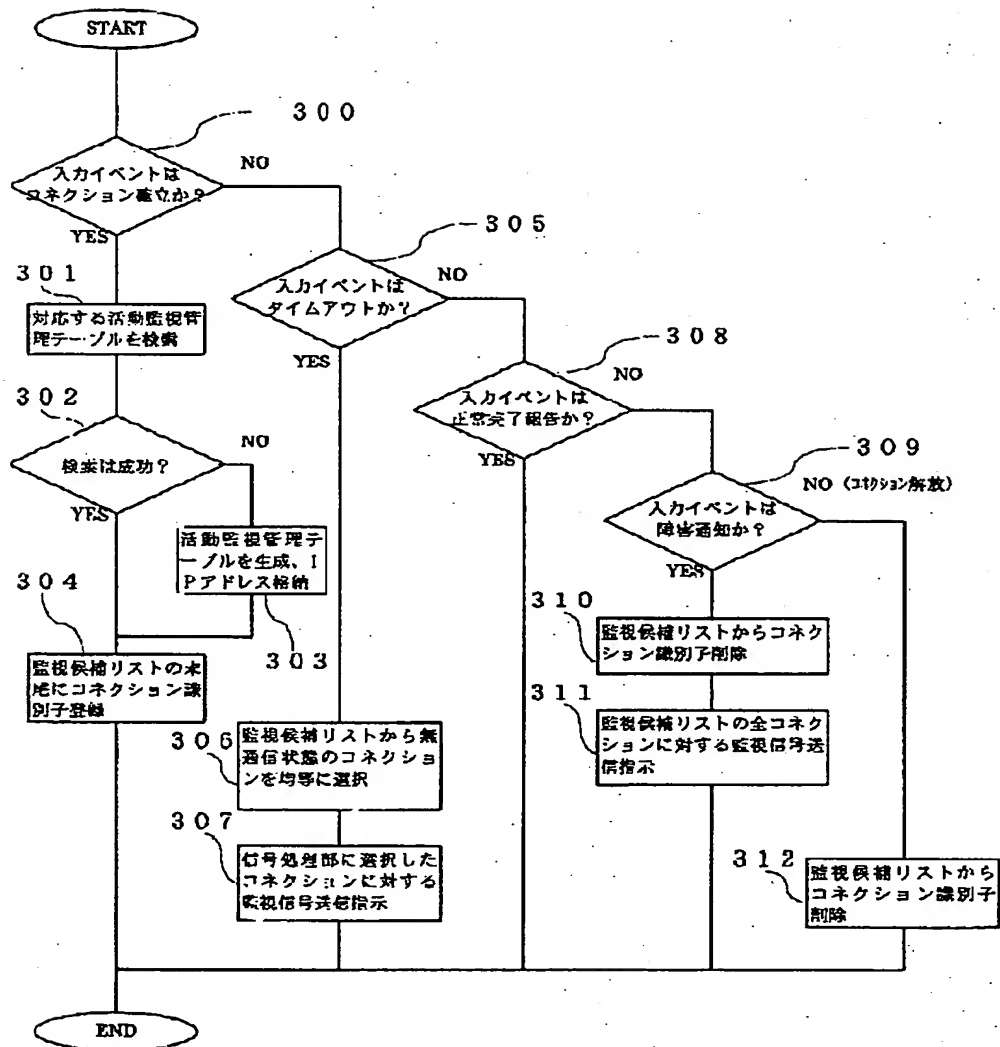
【図2】

図2



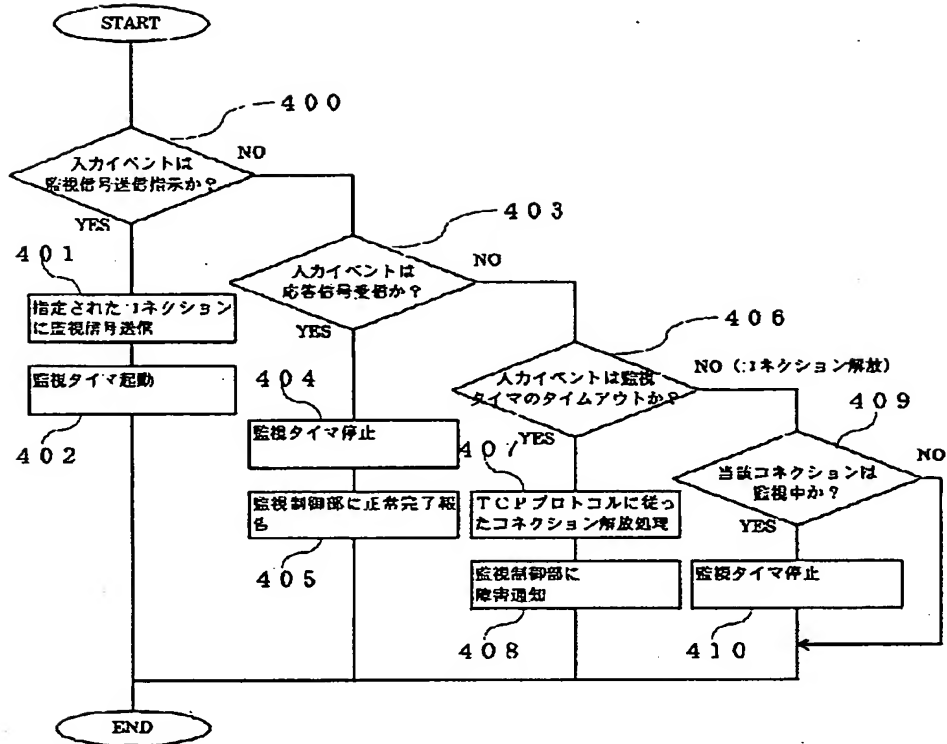
【図3】

図3



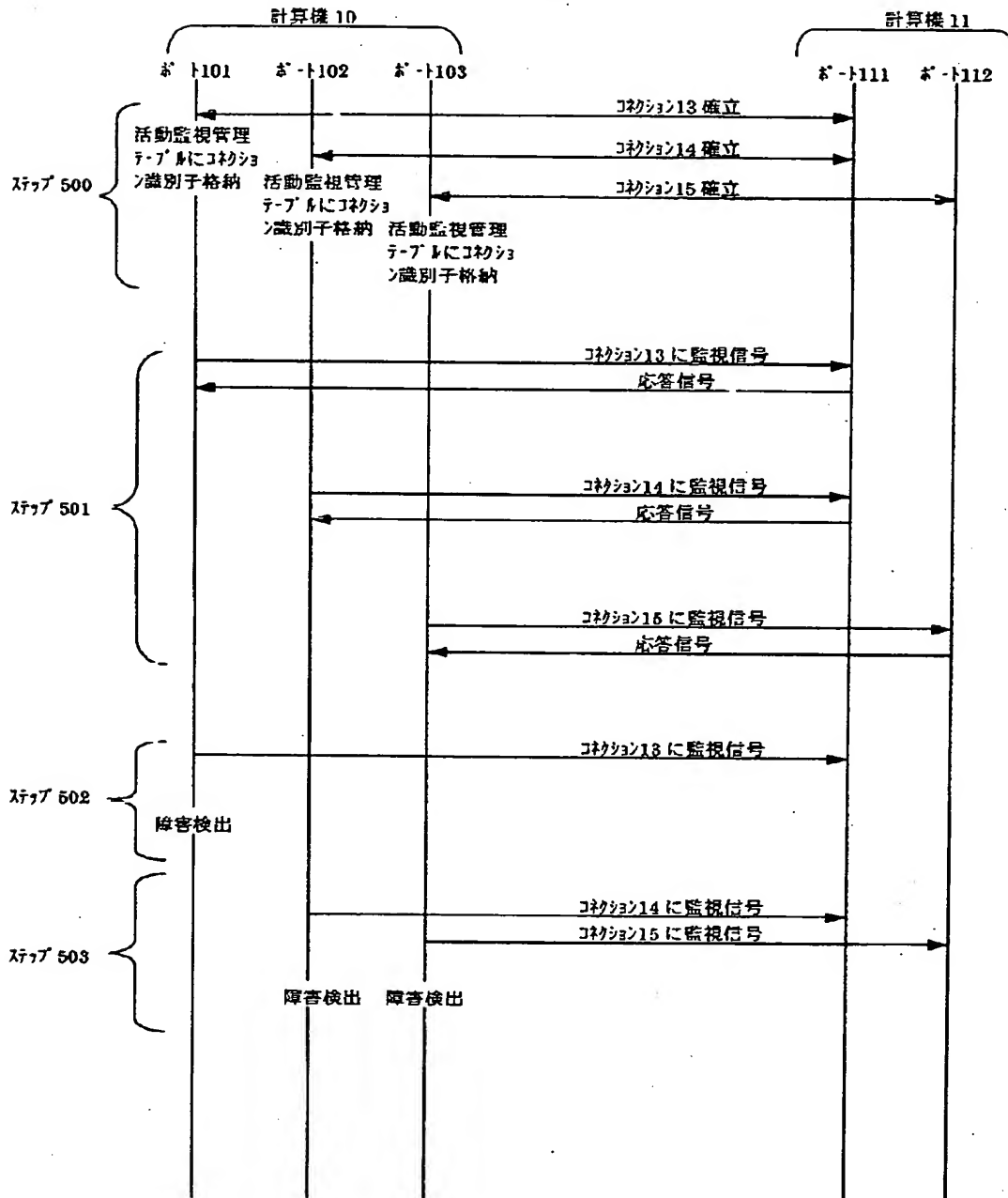
【図4】

図4



【図5】

図5



【図6】

図 6

